Indag. Mathem., N.S., 19 (1), 1–21 March, 2008

Davenport constant for finite abelian groups

by Emre Alkan

Department of Mathematics, Koc University, Rumelifeneri Yolu, 34450, Sariyer, Istanbul, Turkey

Communicated by Prof. R. Tijdeman

ABSTRACT

For a finite abelian group G, we investigate the length of a sequence of elements of G that is guaranteed to have a subsequence with product identity of G. In particular, we obtain a bound on the length which takes into account the repetitions of elements of the sequence, the rank and the invariant factors of G. Consequently, we see that there are plenty of such sequences whose length could be much shorter than the best known upper bound for the Davenport constant of G, which is the least integer s such that any sequence of length s in G necessarily contains a subsequence with product identity. We also show that the Davenport constant for the multiplicative group of reduced residue classes modulo n is comparatively large with respect to the order of the group, which is $\phi(n)$, when n is in certain thin subsets of positive integers. This is done by studying the Carmichael's lambda function, defined as the maximal multiplicative order of any reduced residue modulo n, along these subsets.

1 INTRODUCTION

Let G be a finite abelian group with multiplication. Davenport's constant $D(G)$ is defined to be the least positive integer s such that any sequence (with possible repetitions) of s elements of G contains a subsequence whose product is the identity of G. Historically, $D(G)$ was first introduced by Davenport [6], who obtained a number of interesting results concerning this constant. In particular, he showed that if K is an algebraic number field and G is the ideal class group

MSC: 11N25, 11B75, 20K01

Key words and phrases: Davenport's constant, Carmichael's lambda function, Sequences with repetitions, Finite abelian groups, Invariant factors, Rank, Reduced residues

E-mail: ealkan@ku.edu.tr (E. Alkan).

of K, then $D(G)$ turns out to be the maximal number of prime ideals (counting multiplicity) that appear in the decomposition of an irreducible integer in K. Because of this striking feature of $D(G)$ and other implications, it is of great interest to have the best possible bounds for this combinatorial invariant. As a consequence of the Fundamental Theorem for finite abelian groups, one has $G = \mathbb{M}_{n_1} \times \mathbb{M}_{n_2} \times \cdots \times \mathbb{M}_{n_d}$ where $n_1, n_2, \ldots, n_d$ are the unique integers known as the invariant factors of G satisfying $2 \leqslant n_1 | n_2 | \cdots | n_{d-1} | n_d$ and $\mathbb{M}_n$ is the cyclic group of order n. Here d is the rank of G and n_d is the maximum possible order of an element of G. Let us denote by

$$M(G) = 1 + \sum_{j=1}^{d} (n_j - 1).$$

If $\mathbb{M}_{n_j}$ is generated by h_j for $1 \leqslant j \leqslant d$, then the sequence

$$\langle h_1, h_1, \ldots, h_1, h_2, h_2, \ldots, h_2, \ldots, h_d, h_d, \ldots, h_d \rangle,$$

where each h_j repeats exactly $n_j - 1$ times, has no subsequence with product identity so that $n_d \leqslant M(G) \leqslant D(G)$. Note that $M(G) \leqslant \sigma(n_d) = O(n_d \log\log n_d)$ where $\sigma(n_d)$ is the sum of all divisors of n_d. Consequently it is not a significant loss if n_d is used as a lower bound for $D(G)$ instead of $M(G)$. We also have the bound $D(G) \leqslant |G|$ and these bounds are tight for cyclic groups. If H is a subgroup of G, then one can show that $D(H) \leqslant D(G)$. Olson [29,30] proved that $D(G) = M(G)$ for all finite abelian groups of rank 2 and for all finite abelian p-groups. Geroldinger and Schneider [16] proved that the possibility $D(G) > M(G)$ occurs rather frequently. The question of whether $M(G) = D(G)$ holds for finite abelian groups of rank 3 was first studied by Van Emde Boas [36] and recently Gao [14] made important progress towards its solution. For a variety of other interesting results about $D(G)$ for special types of finite abelian groups the reader may consult [4,5,7,15,24,34]. It is also conjectured that (see [27])

$$D(G) \leqslant \sum_{j=1}^{d} n_j.$$

Longest possible sequences in G with no nonempty subsequence having product identity played a key role in the celebrated proof of the infinitude of Carmichael numbers by Alford, Granville and Pomerance [1]. Therefore, obtaining good upper bounds for the Davenport constant constitutes an important problem in combinatorial number theory with many applications. Currently the best upper bound for $D(G)$ is due to Van Emde Boas and Kruyswijk [37] and Meshulam [25] (see also [1] and [2]) who proved that

$$D(G) \leqslant n + \left\lceil n \log\left(\frac{|G|}{n}\right)\right\rceil.$$

where n is the maximum possible order of an element also known as the exponent of the group. For some special types of nonabelian finite p-groups upper bounds for $D(G)$ were obtained by Dimitrov [8].

It would be desirable to have results on the length of sequences that are guaranteed to have a subsequence with product identity which takes into account the repetitions of elements of the sequence, the rank and the invariant factors of G. Note that given $g \in G$, the order of g divides n_d, so that choosing a minimal invariant factor n_j with the order of g dividing n_j, we see that there is an invariant factor n_j having the property that the order of g divides n_j but does not divide any other invariant factor which is strictly smaller than n_j. With this observation in mind, our goal is to prove the following result:

Theorem 1. *Let G be a finite abelian group of rank d with invariant factors $2 \leqslant n_1|n_2|\cdots|n_{d-1}|n_d = n$. Consider the sequence of elements of G,*

$$L = \langle g_1, g_1, \ldots, g_1, g_2, g_2, \ldots, g_2, \ldots, g_d, g_d, \ldots, g_d, s_1, s_2, \ldots, s_r \rangle$$

with distinct $g_1, g_2, \ldots, g_d$ where for each $1 \leqslant j \leqslant d$, g_j appears $n_j - k_j$ times with $1 \leqslant k_j \leqslant n_j$, (if $n_j = k_j$, then g_j does not appear in the sequence) the order of g_j divides n_j but does not divide any other invariant factor which is strictly smaller than n_j and $s_1, s_2, \ldots, s_r$ are arbitrary elements of G such that

$$r = n + \max\left(0, \left[n \log\left(\frac{|G|}{n} \prod_{j=1}^{d} \frac{k_j}{n_j}\right)\right]\right).$$

Then L has a subsequence whose product is the identity of G.

As our next result clearly demonstrates, for finite abelian groups with large rank, there are plenty of shorter sequences that are guaranteed to have a subsequence with product identity of G.

Corollary 1. *Let G be a finite abelian group of rank $d \geqslant 2$ with invariant factors $2 \leqslant n_1|n_2|\cdots|n_{d-1}|n_d = n$. Let S be a subset of $\{1, 2, \ldots, d-1\}$ and L be a sequence in G such that for each n_j with $j \in S$, L contains distinct elements g_j where the order g_j divides n_j but does not divide any other invariant factor which is strictly smaller than n_j. If the length of L is denoted by $|L|$ and*

$$|L| \geqslant n + \left[n \log\left(\frac{|G|}{n}\right)\right] - \left[\sum_{j \in S}\left(\frac{n}{2(n_j - 1)} - 1\right)\right],$$

(empty sums are assumed to be zero) then L contains a subsequence with product identity of G.

An application of Corollary 1 can be given for the multiplicative group of all reduced residue classes modulo m, denoted as $(\mathbb{Z}/m\mathbb{Z})^* = \mathbb{Z}_m{}^*$. In the next section,

we present numerical examples for these groups which illustrate the lower bound computed for the length of the sequence described in Corollary 1 that is guaranteed to have a subsequence with product congruent to 1 modulo m. If p is prime and $k \geqslant 1$, then by Dirichlet's theorem, there are infinitely many primes q satisfying $q \equiv 1 \pmod{p^k}$ so that $|\mathbb{Z}_q{}^*| = q - 1$ is divisible by p^k. Since $\mathbb{Z}_q{}^*$ is cyclic, the cyclic group of order p^k namely $\mathbb{M}_{p^k}$ is a subgroup of $\mathbb{Z}_q{}^*$. Using the Fundamental Theorem on finite abelian groups and the Chinese Remainder theorem, it follows that any finite abelian group can be realized as a subgroup of some $\mathbb{Z}_h{}^*$ with square-free h. Moreover using Dirichlet's theorem repeatedly, one can find a square-free number h such that the direct product $\mathbb{M}_p \times \mathbb{M}_{p^2} \times \cdots \times \mathbb{M}_{p^k}$ is a subgroup of $\mathbb{Z}_h{}^*$ and therefore the p-rank of $\mathbb{Z}_h{}^*$ is at least k. Consequently one can find $\mathbb{Z}_h{}^*$ of arbitrarily large rank. Therefore, if G is a finite abelian group and a subgroup of $\mathbb{Z}_h{}^*$ for some square-free h, then $D(G) \leqslant D(\mathbb{Z}_h{}^*)$ and the groups $\mathbb{Z}_h{}^*$ can be viewed as universal in this sense. Moreover, if $G = \mathbb{Z}_m^*$ for some $m > 1$, then the maximal invariant factor of G is known as the Carmichael's lambda function $\lambda(m)$, defined as the maximal multiplicative order of any reduced residue modulo m which turns out to be the least common multiple of all $\lambda(p^r)$ over the prime powers p^r exactly dividing m. It is well known that $\lambda(p^r) = \phi(p^r)$ for all prime powers p^r, except the case $p = 2$ and $r \geqslant 3$ where one has $\lambda(2^r) = \frac{1}{2}\phi(2^r)$. A remarkable study of $\lambda(m)$ was done by Erdös, Pomerance and Schmutz [11]. They proved, among other results, that

$$\lambda(m) > \frac{m}{(\log m)^{\log\log\log m + A + o(1)}}$$

for almost all m, where A is an explicitly defined constant and the $o(1)$ term is shown to be $\ll (\log\log m)^{-1+\epsilon}$ for every fixed $\epsilon > 0$. Moreover, they consider $\lambda(m)$ on the average obtaining the estimate

$$\sum_{m \leqslant x} \lambda(m) = \frac{x^2}{\log x} \exp\left(\frac{B \log\log x}{\log\log\log x} \big(1 + o(1)\big) \right),$$

where B is an explicitly defined constant. In an interesting paper, Luca and Sankaranarayanan [22] studied all moments of $\lambda(m)$ and proved for $r > 0$ that

$$\sum_{m \leqslant x} \lambda(m)^r = \frac{x^{r+1}}{\log x} \exp\left(\frac{B_r \log\log x}{\log\log\log x} \big(1 + o(1)\big) \right)$$

for a certain constant B_r. They also consider the more subtle problem of negative moments of $\lambda(m)$ obtaining the lower bound

$$\sum_{m \leqslant x} \lambda(m)^r \geqslant x^{1-\delta+o(1)}$$

for a constant $\delta > 0$ which turns out to be related to the distribution of primes p such that $p - 1$ is a smooth number. The average multiplicative order of elements

modulo m was nicely treated by Luca and Shparlinski [23]. A problem about the local behavior of Carmichael's lambda function was solved by Doyon and Luca [9]. Recently, Ford and Hu [13] obtained results on the distribution of divisors of $\lambda(m)$ inspired by the techniques that Ford [12] introduced in his impressive work on the distribution of integers with a divisor in a specified interval. Using the fact that $n_d \leqslant D(G)$, we have $\lambda(m) \leqslant D(\mathbb{Z}_m^*)$. Combining this with the above estimate of Erdös, Pomerance and Schmutz, we see that

$$D(\mathbb{Z}_m^*) > \frac{m}{(\log m)^{\log\log\log m + A + o(1)}}$$

holds for almost all m. This shows that, for almost all m, the Davenport constant of $\mathbb{Z}_m^*$ is comparatively large with respect to the order of the group $\phi(m) = |\mathbb{Z}_m^*|$. Our result below indicates that the Davenport constant of $\mathbb{Z}_m^*$ is even larger compared to the order of the group when m comes from certain thin subsets consisting of integers with few prime divisors. The precise formulation of our claim is as follows.

Theorem 2. *Consider the set of integers*

$$S_K(x) = \{n \leqslant x \ : \ \Omega(n) \leqslant K\}$$

for a fixed integer K, where $\Omega(n)$ is the total number of prime factors of n counting multiplicity. Then for almost all $n \in S_K(x)$ and every fixed $\epsilon > 0$, we have

$$D(\mathbb{Z}_n^*) \geqslant \frac{n}{(\log n)^{(\frac{K}{2})+2+\epsilon}},$$

where the number of exceptions depends only on K and ϵ. Moreover let $h(x)$ be a monotonically increasing function tending to infinity such that $h(x) = o(\log\log x)$ and for every fixed $c > 1$,

$$\frac{h(x)}{h(\sqrt{x})} \leqslant c$$

when x is sufficiently large in terms of c. If we consider the set of integers

$$S_h(x) = \{n \leqslant x \ : \ \Omega(n) \leqslant h(x)\},$$

then for almost all $n \in S_h(x)$ and every fixed $\epsilon > 0$, one has

$$D(\mathbb{Z}_n^*) \geqslant \frac{n}{(\log n)^{(\frac{1}{2}+\epsilon)h^2(n)}},$$

where the number of exceptions depends only on $h(x)$ and ϵ.

We remark that almost all integers $n \leqslant x$ have about $\log\log x$ prime factors (even with counting multiplicity) by a classical theorem of Hardy and Ramanujan [19]. Hence the sets $S_h(x)$ of the above theorem clearly satisfy $S_h(x) = o(x)$. It follows

that the smaller $h(x)$ we take, the thinner these sets $S_h(x)$ will be, but at the same time the lower bound obtained for $D(\mathbb{Z}_n^*)$ becomes superior to the lower bound obtained above as a direct consequence of the estimate of Carmichael's lambda function for almost all n by Erdös, Pomerance and Schmutz. In particular we may take $h(x) = \log_j x = \log_{j-1}(\log x)$ as the j-th iterated logarithm for $j \geqslant 3$, which is easily seen to satisfy the hypotheses of Theorem 2, to obtain that

$$D(\mathbb{Z}_n^*) \geqslant \frac{n}{(\log n)^{(\frac{1}{2}+\epsilon)(\log_j n)^2}}$$

for every fixed $\epsilon > 0$ and for almost all $n \in S_h(x)$. Our next result confirms that the normal order of the quotient $\frac{D(\mathbb{Z}_n^*)}{\lambda(n)}$ is rather small.

Theorem 3. *For almost all $n \leqslant x$, we have*

$$\frac{D(\mathbb{Z}_n^*)}{\lambda(n)} = O(\log\log x \cdot \log\log\log x).$$

For almost all $n \in S_h(x)$, we have

$$\frac{D(\mathbb{Z}_n^*)}{\lambda(n)} = O\big(h^2(x)\log\log x\big).$$

For almost all $n \in S_K(x)$, we have

$$\frac{D(\mathbb{Z}_n^*)}{\lambda(n)} = O_K(\log\log x).$$

Our final result is concerned about the average behavior of the quotient $\frac{D(\mathbb{Z}_n^*)}{\lambda(n)}$.

Theorem 4. *For all $x > e$, we have*

$$\sum_{n\leqslant x} \frac{D(\mathbb{Z}_n^*)}{\lambda(n)} = O\big(x(\log\log x)^3\big).$$

We remark that $\sum_{n\leqslant x} \frac{D(\mathbb{Z}_n^*)}{\lambda(n)}$ is clearly $\gg x$. It would be an interesting problem to find nontrivial lower bounds and the true order of growth of this sum.

2 EXAMPLES

In this section, we present two examples illustrating Corollary 1. As our first example, we take $m = 5^3 \cdot 7^4 \cdot 11^3$ so that $|\mathbb{Z}_m^*| = \phi(m) = 2^4 \cdot 3 \cdot 5^3 \cdot 7^3 \cdot 11^2 = 249018000$. It is easy to see that

$$\mathbb{Z}_m^* = \mathbb{Z}_{5^3}^* \times \mathbb{Z}_{7^4}^* \times \mathbb{Z}_{11^3}^* = \mathbb{M}_{2^2\,5^2} \times \mathbb{M}_{2\,3\,7^3} \times \mathbb{M}_{2\,5\,11^2}.$$

It follows that

$$\mathbb{Z}_m^* = \mathbb{M}_2 \times (\mathbb{M}_2 \times \mathbb{M}_5) \times (\mathbb{M}_{2^2} \times \mathbb{M}_3 \times \mathbb{M}_{5^2} \times \mathbb{M}_{7^3} \times \mathbb{M}_{11^2}).$$

Therefore the rank of this group is 3 with invariant factors $n_1 = 2$, $n_2 = 2.5 = 10$ and $n_3 = 2^2 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot 11^2 = 12450900$. Using these values the upper bound for the Davenport constant is computed to be

$$n_3 + \left\lceil n_3 \log\left(\frac{|\mathbb{Z}_m^*|}{n_3}\right)\right\rceil = 12450900 + 37299562 = 49750462.$$

To apply Corollary 1, assume that $S = \{1, 2\}$ and let L be a sequence of elements in the group such that for $j = 1, 2$, L contains distinct elements g_j where the order of g_j divides n_j but does not divide strictly smaller invariant factors. If the length of L satisfies

$$\begin{aligned} |L| &\geqslant 49750462 - \left\lceil \left(\frac{2^2 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot 11^2}{2 \cdot 9} - 1\right) + \left(\frac{2^2 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot 11^2}{2} - 1\right)\right\rceil \\ &= 49750462 - 6917164 = 42833298, \end{aligned}$$

then L is guaranteed to have a subsequence with product congruent to 1 modulo m. For the second example, we take $m = 5^3 \cdot 7^4 \cdot 11^3 \cdot 13^2$ so that $|\mathbb{Z}_m^*| = 2^6 \cdot 3^2 \cdot 5^3 \cdot 7^3 \cdot 11^2 \cdot 13 = 38846808000$. We then have,

$$\mathbb{Z}_m^* = \mathbb{M}_2 \times \mathbb{M}_2 \times (\mathbb{M}_{2^2} \times \mathbb{M}_3 \times \mathbb{M}_5) \times (\mathbb{M}_{2^2} \times \mathbb{M}_3 \times \mathbb{M}_{5^2} \times \mathbb{M}_{7^3} \times \mathbb{M}_{11^2} \times \mathbb{M}_{13}).$$

This group has rank 4 and the invariant factors are $n_1 = n_2 = 2$, $n_3 = 2^2 \cdot 3 \cdot 5 = 60$ and $n_4 = 2^2 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot 11^2 \cdot 13 = 161861700$. With these values we compute the upper bound for the Davenport constant as

$$n_4 + \left\lceil n_4 \log\left(\frac{|\mathbb{Z}_m^*|}{n_4}\right)\right\rceil = 161861700 + 887105533 = 1048967233.$$

Assuming $S = \{1, 2, 3\}$, if L is a sequence of elements in the group such that for $j = 1, 2, 3$, L contains distinct elements g_j where the order of g_j divides n_j but does not divide strictly smaller invariant factors, then L contains a subsequence with product congruent to 1 modulo m provided

$$\begin{aligned} |L| &\geqslant 1048967233 - \left\lceil \sum_{j=1}^{3} \frac{n_4}{2(n_j - 1)} - 1 \right\rceil \\ &= 1048967233 - 163233406 = 885733827. \end{aligned}$$

3 PROOF OF THEOREM 1

Assume that the sequence

$$L = \langle g_1, g_1, \ldots, g_1, g_2, g_2, \ldots, g_2, \ldots, g_d, g_d, \ldots, g_d, s_1, s_2, \ldots, s_r \rangle$$

is given with distinct $g_1, g_2, \ldots, g_d$ where for each $1 \leqslant j \leqslant d$, g_j appears $n_j - k_j$ times with $1 \leqslant k_j \leqslant n_j$, the order of g_j divides n_j but does not divide any other

invariant factor which is strictly smaller than n_j and $s_1, s_2, \ldots, s_r$ are arbitrary elements of G such that

$$r = n + \left[n \log \left(\frac{|G|}{n} \prod_{j=1}^{d} \frac{k_j}{n_j} \right) \right].$$

We modify the method introduced in [1]. First, let us take a prime q such that $q \equiv 1 \pmod{n}$. Consider the group ring $\mathbb{F}_q[G]$ where $\mathbb{F}_q$ is the field with q elements. It is sufficient to find nonzero elements

$$a_{11}, a_{12}, \ldots, a_{1(n_1-k_1)}, a_{21}, a_{22}, \ldots, a_{2(n_2-k_2)}, \ldots, a_{d1}, a_{d2}, \ldots, a_{d(n_d-k_d)},$$
$$b_1, b_2, \ldots, b_r$$

in $\mathbb{F}_q$ such that the product

$$(1) \qquad \prod_{j=1}^{n_1-k_1} (g_1 - a_{1j}) \cdot \prod_{j=1}^{n_2-k_2} (g_2 - a_{2j}) \cdots \prod_{j=1}^{n_d-k_d} (g_d - a_{dj}) \cdot \prod_{j=1}^{r} (s_j - b_j)$$

is null, since if L has no subsequence with product identity, then the constant term in the expansion of this product in $\mathbb{F}_q[G]$ would be

$$\prod_{j=1}^{n_1-k_1} a_{1j} \cdot \prod_{j=1}^{n_2-k_2} a_{2j} \cdots \prod_{j=1}^{n_d-k_d} a_{dj} \cdot \prod_{j=1}^{r} b_j = 0$$

which is a contradiction. Using extensions of all the group characters (there are exactly $|G|$ such characters) $\chi : G \to \mathbb{F}_q^*$ ($\mathbb{F}_q^*$ denotes the multiplicative group in $\mathbb{F}_q$) to ring homomorphisms $\chi : \mathbb{F}_q[G] \to \mathbb{F}_q$ and orthogonality of these characters, for the above product (1) to be zero, it suffices to show that for each extended group character χ either $\chi(g_t) = a_{tj}$ or $\chi(s_j) = b_j$ for some a_{tj} or b_j. Hence our strategy is to cover as many characters as we can and choose the remaining (if any exist) elements in an arbitrary manner. Let us consider g_1. Since the order of g_1 is a divisor of n_1, $\chi(g_1)$ is an n_1th root of unity in $\mathbb{F}_q^*$ for any character χ. Hence there is $a_{11} \in \mathbb{F}_q^*$ such that

$$\#\{\chi : \chi(g_1) = a_{11}\} \geqslant \frac{|G|}{n_1}.$$

It follows that

$$\#\{\chi : \chi(g_1) \neq a_{11}\} \leqslant |G| \left(1 - \frac{1}{n_1}\right).$$

Note that if χ is any character such that $\chi(g_1) \neq a_{11}$, then $\chi(g_1)$ is some other n_1th root of unity in $\mathbb{F}_q^*$ and consequently there is $a_{12} \in \mathbb{F}_q^*$ such that

$$\#\{\chi : \chi(g_1) \neq a_{11}, \chi(g_1) = a_{12}\} \geqslant \frac{1}{(n_1 - 1)} \#\{\chi : \chi(g_1) \neq a_{11}\}$$

and

$$\begin{aligned}
&\#\{\chi \,:\, \chi(g_1) \neq a_{11}, \chi(g_1) \neq a_{12}\} \\
&\leqslant \left(1 - \frac{1}{n_1 - 1}\right)\#\{\chi \,:\, \chi(g_1) \neq a_{11}\} \\
&\leqslant |G|\left(1 - \frac{1}{n_1}\right)\left(1 - \frac{1}{n_1 - 1}\right).
\end{aligned}$$

Clearly we can continue in this way until all g_1's are consumed in the given sequence to obtain

$$\#\{\chi \,:\, \chi(g_1) \neq a_{1j}, 1 \leqslant j \leqslant n_1 - k_1\} \leqslant |G| \prod_{j=0}^{n_1 - k_1 - 1}\left(1 - \frac{1}{n_1 - j}\right) = |G|\frac{k_1}{n_1}. \tag{2}$$

Repeating this process for $g_2, \ldots, g_d$, we have

$$\#\{\chi \,:\, \chi(g_i) \neq a_{ij}, 1 \leqslant i \leqslant d, 1 \leqslant j \leqslant n_i - k_i\} \leqslant |G| \prod_{j=1}^{d}\frac{k_j}{n_j}. \tag{3}$$

Note that for the remaining elements $s_1, s_2, \ldots, s_r$, all of $\chi(s_1), \chi(s_2), \ldots, \chi(s_r)$ are nth roots of unity in $\mathbb{F}_q{}^*$. Hence applying the same reasoning to $s_1, s_2, \ldots, s_k$ with

$$k = 1 + \left[n \log\left(\frac{|G|}{n}\prod_{j=1}^{d}\frac{k_j}{n_j}\right)\right] \tag{4}$$

gives

$$\begin{aligned}
&\#\{\chi \,:\, \chi(g_i) \neq a_{ij}, 1 \leqslant i \leqslant d, 1 \leqslant j \leqslant n_i - k_i, \chi(s_v) \neq b_v, 1 \leqslant v \leqslant k\} \\
&\qquad \leqslant |G|\left(\prod_{j=1}^{d}\frac{k_j}{n_j}\right)\left(1 - \frac{1}{n}\right)^k.
\end{aligned} \tag{5}$$

Moreover using (4) we have

$$\left(1 - \frac{1}{n}\right)^k < \exp\left(\frac{-k}{n}\right) \leqslant \exp\left(-\log\left(\frac{|G|}{n}\prod_{j=1}^{d}\frac{k_j}{n_j}\right)\right) = \frac{n}{|G|}\prod_{j=1}^{d}\frac{n_j}{k_j}. \tag{6}$$

Combining (5) and (6), it follows that the number of extended characters of G still not covered by the above process is $\leqslant n - 1$. We denote these remaining characters by $\chi_1, \chi_2, \ldots, \chi_u$ with $u \leqslant n - 1$. Note that $r - k = n - 1$ and we may take $\chi_1(s_{k+1}) = b_{k+1}, \chi_2(s_{k+2}) = b_{k+2}, \ldots, \chi_u(s_{k+u}) = b_{k+u}$. The remaining b_j's (if any exist) can be chosen in an arbitrary manner. To complete the proof we remark that since

$$\frac{|G|}{n}\prod_{j=1}^{d}\frac{k_j}{n_j} = \frac{1}{n}\prod_{j=1}^{d}k_j,$$

one has to take $k = 1$ and $r = n$ when

$$\log\left(\frac{|G|}{n}\prod_{j=1}^{d}\frac{k_j}{n_j}\right) \leqslant 0.$$

This completes the proof of Theorem 1. □

4 REMARKS

Note that the length of the sequence considered in Theorem 1 is

$$|L| = n + \left(\sum_{j=1}^{d}(n_j - k_j)\right) + \left[n\log\left(\frac{|G|}{n}\prod_{j=1}^{d}\frac{k_j}{n_j}\right)\right]. \tag{7}$$

For any positive integer n, the function $f(x) = n\log x - x$ is strictly increasing for $0 < x < n$. Using this, let us see that

$$|L| \leqslant n + \left[n\log\left(\frac{|G|}{n}\right)\right]. \tag{8}$$

Clearly we have

$$\begin{aligned} |L| &= n + \left(\sum_{j=1}^{d}(n_j - k_j)\right) + \left[n\log\left(\frac{|G|}{n}\right) - n\sum_{j=1}^{d}(\log n_j - \log k_j)\right] \\ &\leqslant n + \left(\sum_{j=1}^{d}(n_j - k_j)\right) + \left[n\log\left(\frac{|G|}{n}\right)\right] - \left[n\sum_{j=1}^{d}(\log n_j - \log k_j)\right]. \end{aligned} \tag{9}$$

If $n_j = k_j$ for some j, then g_j gives no contribution to $|L|$. Therefore we may consider only terms with $1 \leqslant k_j \leqslant n_j - 1$. Since $f(x)$ is strictly increasing for $0 < x < n$, we obtain that $n_j - k_j < n(\log n_j - \log k_j)$ and

$$\sum_{j=1}^{d}(n_j - k_j) < n\sum_{j=1}^{d}(\log n_j - \log k_j). \tag{10}$$

Since left hand side of (10) is an integer, it follows from (10) that

$$\sum_{j=1}^{d}(n_j - k_j) \leqslant \left[n\sum_{j=1}^{d}(\log n_j - \log k_j)\right]. \tag{11}$$

Combining (9) and (11) we deduce (8) as claimed. Let us now look at some extreme cases. First of all if we do not exploit possible repetitions in our sequence, then this amounts to taking $n_j = k_j$ for all j and (8) reduces to the bound

$$D(G) \leqslant n + \left[n\log\left(\frac{|G|}{n}\right)\right]$$

mentioned in the introduction. On the other hand, taking $k_j = 1$ for all j so that each g_j appears a maximum possible number of $n_j - 1$ times in L and noticing that

$$\log\left(\frac{|G|}{n}\prod_{j=1}^{d}\frac{k_j}{n_j}\right) = -\log n \leqslant 0,$$

we have

$$|L| = n + \sum_{j=1}^{d}(n_j - 1),$$

which shows the decrease in the length due to repetitions. On the other extreme taking $k_j = n_j - 1$ for all j, so that each g_j appears only once in L gives a dramatic increase in the length as

$$|L| = d + n + \left[n\log\left(\frac{|G|}{n}\prod_{j=1}^{d}\left(1 - \frac{1}{n_j}\right)\right)\right].$$

Finally taking $k_j = n_j$ for $1 \leqslant j \leqslant d-1$ and $k_d = n_d - 1$ gives

$$|L| = 1 + n + \left[n\log\left(\frac{|G|}{n}\left(1 - \frac{1}{n}\right)\right)\right].$$

Since $n\log(1 - \frac{1}{n})$ approaches to -1 as n tends to infinity, this almost agrees with the bound for $D(G)$ mentioned in the introduction.

5 PROOF OF COROLLARY 1

Let L be a given sequence in G such that for each invariant factor n_j with $j \in S$, L contains distinct elements g_j where the order of g_j divides n_j but does not divide any other invariant factor which is strictly smaller than n_j and

$$|L| \geqslant n + \left[n\log\left(\frac{|G|}{n}\right)\right] - \left[\sum_{j\in S}\left(\frac{n}{2(n_j - 1)} - 1\right)\right]. \tag{12}$$

By Theorem 1, if the length of L is

$$\geqslant n + \left(\sum_{j=1}^{d}(n_j - k_j)\right) + \left[n\log\left(\frac{|G|}{n}\prod_{j=1}^{d}\frac{k_j}{n_j}\right)\right], \tag{13}$$

then L has a subsequence with product identity. Consider the quantity

$$\left[n\sum_{j=1}^{d}(\log n_j - \log k_j)\right] - \left(\sum_{j=1}^{d}(n_j - k_j)\right). \tag{14}$$

Since the function

$$g(x) = n\log\left(1+\frac{1}{x}\right) - 1 = n\log(x+1) - x - 1 - (n\log x - x)$$

is strictly decreasing for $x > 0$ and by our assumption $1 \leqslant k_j \leqslant n_j - 1$ for all $j \in S$, we see that $n(\log n_j - \log k_j) - (n_j - k_j)$ is minimized if we take $k_j = n_j - 1$. Moreover the minimum value is

$$n\log\left(\frac{n_j}{n_j-1}\right) - 1 = n\log\left(1+\frac{1}{n_j-1}\right) - 1. \tag{15}$$

Using the Taylor expansion of $\log(1+z)$ we see that the right side of (15) is

$$\geqslant n\left(\frac{1}{(n_j-1)} - \frac{1}{2(n_j-1)^2}\right) - 1 \geqslant \frac{n}{2(n_j-1)} - 1 > 0 \tag{16}$$

for all $j \in S$. Using the fact that $n(\log n_j - \log k_j) - (n_j - k_j) \geqslant 0$ for any $1 \leqslant j \leqslant d$ and summing over all j, it follows from (16) that

$$n\sum_{j=1}^{d}(\log n_j - \log k_j) - \left(\sum_{j=1}^{d}(n_j - k_j)\right) \geqslant \sum_{j\in S}\left(\frac{n}{2(n_j-1)} - 1\right). \tag{17}$$

Combining (14) and (17) one sees that

$$\left[n\sum_{j=1}^{d}(\log n_j - \log k_j)\right] - \left(\sum_{j=1}^{d}(n_j - k_j)\right) \geqslant \left[\sum_{j\in S}\left(\frac{n}{2(n_j-1)} - 1\right)\right]. \tag{18}$$

From (9) and (18) we have that

$$\begin{aligned} n + \left(\sum_{j=1}^{d}(n_j - k_j)\right) + \left[n\log\left(\frac{|G|}{n}\prod_{j=1}^{d}\frac{k_j}{n_j}\right)\right] \\ \leqslant n + \left[n\log\left(\frac{|G|}{n}\right)\right] - \left[\sum_{j\in S}\left(\frac{n}{2(n_j-1)} - 1\right)\right]. \end{aligned} \tag{19}$$

Finally using (12), (13) and (19), we complete the proof of Corollary 1. □

6 PROOF OF THEOREM 2

Let us recall that

$$S_h(x) = \{n \leqslant x \,:\, \Omega(n) \leqslant h(x) = o(\log\log x)\}$$

and for any integer $k \geqslant 1$, denote by

$$\Pi_k(x) = |\{n \leqslant x \,:\, \Omega(n) = k\}|.$$

Strong asymptotic formulas are known for $\Pi_k(x)$, in particular we may quote the following result from [35]: Uniformly for $x \geqslant 3$ and $1 \leqslant k \leqslant (2-\delta)\log\log x$ with $0 < \delta < 1$, one has

$$\Pi_k(x) = \frac{x(\log\log x)^{k-1}}{(k-1)!\log x}\left(\nu\left(\frac{k-1}{\log\log x}\right) + O_\delta\left(\frac{k}{(\log\log x)^2}\right)\right). \tag{20}$$

Here the complex function $\nu(z)$ is defined as

$$\nu(z) = \frac{1}{\Gamma(z+1)}\prod_p\left(1-\frac{z}{p}\right)^{-1}\left(1-\frac{1}{p}\right)^z,$$

where the product is taken over all primes, $\Gamma(z)$ is the Gamma function and specially $\nu(0) = 1$. Historically, the origin of these type of results goes back to the classical work of Hardy and Ramanujan [19] and later great uniformity in k were obtained by Sathe [31,32], Erdös [10] and Selberg [33]. Consequently, using (20), for any $1 \leqslant k \leqslant h(x) = o(\log\log x)$, we have

$$\Pi_k(x) = O\left(\frac{x(\log\log x)^{k-1}}{(k-1)!\log x}\right)$$

where the implied constant is absolute. Taking $1+m = [h(x)]$, it follows that

$$\begin{aligned}
\left|S_h(x)\right| &= O\left(\sum_{k\leqslant h(x)}\Pi_k(x)\right) = O\left(\sum_{k\leqslant h(x)}\frac{x(\log\log x)^{k-1}}{(k-1)!\log x}\right)\\
&= O\left(\frac{x(\log\log x)^m}{m!\log x}\left(1+\frac{m}{\log\log x}+\frac{m(m-1)}{(\log\log x)^2}+\cdots+\frac{m!}{(\log\log x)^m}\right)\right)\\
&= O\left(\frac{x(\log\log x)^m}{m!\log x}\left(1+\frac{m}{\log\log x}+\frac{m^2}{(\log\log x)^2}+\cdots+\frac{m^m}{(\log\log x)^m}\right)\right)\\
&= O\left(\frac{x(\log\log x)^m}{m!\log x}\right)
\end{aligned}$$

since the geometric series with common factor $\frac{m}{\log\log x} = o(1)$ converges. Clearly we also have

$$\left|S_h(x)\right| \gg \frac{x(\log\log x)^m}{m!\log x}.$$

Let M be the number of $n \leqslant x$ with a square-full divisor d such that $d > (\log x)^{2+\epsilon}$ for $\epsilon > 0$. It is well known that (see [21]), if $S(y)$ is the number of square-full integers $\leqslant y$, then $S(y) \ll y^{\frac{1}{2}}$. Fixing such a divisor d, the number of $n \leqslant x$ divisible by d is $[\frac{x}{d}] \leqslant \frac{x}{d}$. Therefore by partial summation, we have that

$$M \leqslant x\sum_{\substack{d>(\log x)^{2+\epsilon}\\ d \text{ square-full}}}\frac{1}{d} = S(x) - \frac{S((\log x)^{2+\epsilon})}{(\log x)^{2+\epsilon}} + x\int_{(\log x)^{2+\epsilon}}^{x}\frac{S(t)}{t^2}\,dt. \tag{21}$$

Noting that $S(x) \ll x^{\frac{1}{2}}$, $S((\log x)^{2+\epsilon}) \ll (\log x)^{1+\frac{\epsilon}{2}}$ and

$$\int_{(\log x)^{2+\epsilon}}^{x} \frac{S(t)}{t^2}\, dt \ll \int_{(\log x)^{2+\epsilon}}^{\infty} \frac{1}{t^{\frac{3}{2}}}\, dt \ll (\log x)^{1+\frac{\epsilon}{2}},$$

we obtain from (21) that

$$M \ll \frac{x}{(\log x)^{1+\frac{\epsilon}{2}}} = o\left(\frac{x(\log\log x)^m}{m!\log x}\right) = o\big(S_h(x)\big). \tag{22}$$

From (22), we see that almost all $n \in S_h(x)$ has a large square-free divisor n_1 satisfying

$$n_1 \geqslant \frac{n}{(\log x)^{2+\epsilon}}. \tag{23}$$

Note that for any m relatively prime to n, we have $m^{\lambda(n)} \equiv 1 \pmod{n}$ and $m^{\lambda(n)} \equiv 1 \pmod{n_1}$ since n_1 is a divisor of n. Therefore the order of m modulo n_1 is a divisor of $\lambda(n)$. Since $\lambda(n_1)$ is the least common multiple of orders of all reduced residues modulo n_1, it follows that $\lambda(n_1)$ divides $\lambda(n)$ and in particular that $\lambda(n_1) \leqslant \lambda(n)$. Our next goal is to estimate $\lambda(n_1)$ from below. To this end, let N be the number of $n \leqslant x$ having two prime divisors $p \neq q$ with a divisor d of $(p-1, q-1)$ satisfying $d > (\log x)^{1+\epsilon}$ for $\epsilon > 0$. Given d, p and q, the number of such $n \leqslant x$ is at most $[\frac{x}{pq}] \leqslant \frac{x}{pq}$. Summing up first over p and q while d is fixed and then summing up over d, we obtain that

$$N \leqslant x \sum_{d > (\log x)^{1+\epsilon}} \sum_{\substack{p,q \leqslant x \\ p \equiv 1 \pmod{d} \\ q \equiv 1 \pmod{d}}} \frac{1}{pq} \leqslant \frac{x}{2} \sum_{d > (\log x)^{1+\epsilon}} \left(\sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod{d}}} \frac{1}{p} \right)^2. \tag{24}$$

Let $\pi(x, d, 1)$ be the number of primes $\leqslant x$ that are congruent to 1 modulo d. By the Brun–Titchmarsh theorem (see [17] and [26]), we know for any $d < x$ that

$$\pi(x, d, 1) \leqslant \frac{2x}{\phi(d)\log(\frac{x}{d})}. \tag{25}$$

As a consequence of the Brun–Titchmarsh theorem, using partial summation, it follows from (25) that

$$\sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod{d}}} \frac{1}{p} \ll \frac{\log\log x}{\phi(d)} \tag{26}$$

uniformly for all $d < x$. Combining (24) and (26) and using the estimate

$$\phi(d) \gg \frac{d}{\log\log d},$$

we deduce that

$$(27)\qquad N \ll x(\log\log x)^2 \sum_{d>(\log x)^{1+\epsilon}} \frac{1}{\phi^2(d)} \ll \frac{x(\log\log x)^4}{(\log x)^{1+\epsilon}}$$
$$= o\left(\frac{x(\log\log x)^m}{m!\log x}\right) = o\big(S_h(x)\big).$$

By (27) we may now assume that for almost all $n \in S_h(x)$, one has $(p_i - 1, p_j - 1) \leqslant (\log x)^{1+\epsilon}$ for all primes $p \neq q$ dividing n_1. We can now estimate $\lambda(n_1)$ from below. Using the fact that n_1 is square-free, it follows that $\mathbb{Z}_{n_1}^*$ is a direct product of cyclic groups $\mathbb{Z}_p^*$, each having a generator of order $p-1$, for all primes p dividing n_1. Since $\lambda(n_1)$ is the maximal order among all elements, we see that

$$(28)\qquad \lambda(n_1) \geqslant \frac{\prod_{p|n_1}(p-1)}{\prod_{pq|n_1}(p-1,q-1)},$$

where the products in (28) are taken over prime divisors $p \neq q$. The number of choices for p and q are clearly

$$\leqslant \binom{\omega(n)}{2} \leqslant \binom{\Omega(n)}{2} \leqslant \frac{h^2(x)}{2}$$

so that for almost all $n \in S_h(x)$, we have that

$$(29)\qquad \prod_{pq|n_1}(p-1,q-1) \leqslant (\log x)^{(\frac{1}{2}+\epsilon)h^2(x)}$$

for every fixed $\epsilon > 0$. Combining (28) and (29) and using the bound (see [28] and Theorem 328 in [20])

$$\phi(s) \geqslant \frac{Cs}{\log\log s}$$

for some constant $0 < C < e^{-\gamma}$, where γ is the Euler–Mascheroni constant, we obtain

$$(30)\ \lambda(n) \geqslant \lambda(n_1) \geqslant \frac{\phi(n_1)}{(\log x)^{(\frac{1}{2}+\epsilon)h^2(x)}} \geqslant \frac{Cn_1}{(\log x)^{(\frac{1}{2}+\epsilon)h^2(x)}(\log\log n_1)}$$
$$\geqslant \frac{Cn_1}{(\log x)^{(\frac{1}{2}+\epsilon)h^2(x)}(\log\log x)} \geqslant \frac{n_1}{(\log x)^{(\frac{1}{2}+\epsilon)h^2(x)}} = \frac{n}{\left(\frac{n}{n_1}\right)(\log x)^{(\frac{1}{2}+\epsilon)h^2(x)}},$$

where $\epsilon > 0$ may be different in each occurrence to absorb smaller terms. Combining (23) and (30), we have

$$(31)\qquad \lambda(n) \geqslant \frac{n}{(\log x)^{(\frac{1}{2}+\epsilon)h^2(x)+2+\epsilon}}.$$

Since $h(x)$ monotonically tends to infinity, we obtain from (31) that

$$D(\mathbb{Z}_n^*) \geqslant \lambda(n) \geqslant \frac{n}{(\log x)^{(\frac{1}{2}+\epsilon)h^2(x)}} \tag{32}$$

for every fixed $\epsilon > 0$ and for almost all $n \in S_h(x)$. Finally to eliminate the dependence on x, observe that the number of integers satisfying $n < \sqrt{x}$ is $o(S_h(x))$ and we may assume that $\sqrt{x} \leqslant n \leqslant x$. Hence $\log x \leqslant 2\log n$ and using the hypotheses on $h(x)$, we have that $h^2(x) \leqslant c^2 h^2(\sqrt{x}) \leqslant c^2 h^2(n)$ for $c > 1$ and all sufficiently large x in terms of c. It follows from (32) that

$$D(\mathbb{Z}_n^*) \geqslant \frac{n}{(2\log n)^{(\frac{1}{2}+\epsilon)c^2h^2(n)}} \geqslant \frac{n}{(\log n)^{(\frac{1}{2}+\epsilon)h^2(n)}}$$

for almost all $n \in S_h(x)$ since we can absorb the smaller terms with a different $\epsilon > 0$ and choose c as close as we need to 1. Clearly the number of exceptional $n \leqslant x$ depends only on $h(x)$ and $\epsilon > 0$. This completes the proof in the case of $S_h(x)$. In the case of $S_K(x) = \{n \leqslant x : \Omega(n) \leqslant K\}$, where K is a fixed integer, the argument is the same except at the end that the number of choices for p and q are $\leqslant \binom{K}{2}$ and

$$D(\mathbb{Z}_n^*) \geqslant \lambda(n) \geqslant \frac{n}{(2\log n)^{(1+\epsilon)\binom{K}{2}+2+\epsilon}} \geqslant \frac{n}{(\log n)^{\binom{K}{2}+2+\epsilon}}.$$

where the number of exceptions depends only on K and ϵ. This completes the proof of Theorem 2. □

7 PROOF OF THEOREM 3

For any $n > 1$, we know that

$$\frac{D(\mathbb{Z}_n^*)}{\lambda(n)} \leqslant 1 + \log\left(\frac{|\mathbb{Z}_n^*|}{\lambda(n)}\right) = 1 + \log\left(\frac{\phi(n)}{\lambda(n)}\right). \tag{33}$$

Using the estimate of Erdös, Pomerance and Schmutz [11], we have

$$\lambda(n) > \frac{n}{(\log n)^{\log\log\log n + A + o(1)}} \tag{34}$$

for almost all n. It follows from (34) that

$$\frac{\phi(n)}{\lambda(n)} \leqslant (\log n)^{\log\log\log n + A + o(1)} \tag{35}$$

for almost all n. Combining (33) and (35), we obtain

$$\frac{D(\mathbb{Z}_n^*)}{\lambda(n)} = O(\log\log n \cdot \log\log\log n) = O(\log\log x \cdot \log\log\log x)$$

for almost all $n \leqslant x$.

We have, by the proof of Theorem 2, that for almost all $n \in S_h(x)$ (or $n \in S_K(x)$), n has a square-free divisor n_1 with

$$n_1 \geqslant \frac{n}{(\log x)^{2+\epsilon}}$$

for every fixed $\epsilon > 0$. Moreover for any pair of prime divisors $p \neq q$ of n_1, we have $(p-1, q-1) \leqslant (\log x)^{1+\epsilon}$. Consequently

$$\lambda(n) \geqslant \lambda(n_1) \geqslant \frac{n}{(\log x)^{(\frac{1}{2}+\epsilon)h^2(x)}} \tag{36}$$

for almost all $n \in S_h(x)$ and

$$\lambda(n) \geqslant \lambda(n_1) \geqslant \frac{n}{(\log x)^{(\frac{K}{2})+2+\epsilon}} \tag{37}$$

for almost all $n \in S_K(x)$. we deduce from (33), (36) and (37) that

$$\frac{D(\mathbb{Z}_n^*)}{\lambda(n)} = O\left(\log\left(\frac{\phi(n)}{\lambda(n)}\right)\right) = O\left(h^2(x)\log\log x\right)$$

for almost all $n \in S_h(x)$ and

$$\frac{D(\mathbb{Z}_n^*)}{\lambda(n)} = O_K(\log\log x)$$

for almost all $n \in S_K(x)$. This completes the proof of Theorem 3. □

8 PROOF OF THEOREM 4

Using a similar argument as in the proof of Theorem 2, we see that the number of $n \leqslant x$ which are divisible by a square-full number $d > (\log x)^2$ is $O(\frac{x}{\log x})$. Moreover by the Hardy–Ramanujan type inequalities on the number of prime factors of n (see [18] and [35]), we have for a given $\lambda \geqslant 1$ that the number of $n \leqslant x$ with $\omega(n) \geqslant \lambda \log\log x$ is

$$O\left(\frac{x}{(\log x)^{\lambda\log\lambda+1-\lambda}}\right). \tag{38}$$

where $\omega(n)$ is the number of distinct prime factors of n. As a consequence of (38), the number of $n \leqslant x$ with $\omega(n) \geqslant 3\log\log x$ is $O(\frac{x}{\log x})$. We also have from the proof of Theorem 2 that the number of $n \leqslant x$ having prime factors p and q with $(p-1, q-1) > (\log x)^{1+\epsilon}$ for $\epsilon > 0$ is $O(\frac{x}{\log x})$. If A is the set of all $n \leqslant x$ satisfying at least one of the above conditions, then using the fact that

$$\log\left(\frac{\phi(n)}{\lambda(n)}\right) \leqslant \log x$$

we obtain

$$\sum_{n\in A}\log\left(\frac{\phi(n)}{\lambda(n)}\right)=O(x). \tag{39}$$

On the other hand, if $n\leqslant x$ and n is not in A, then we may write $n=n_1\cdot(\frac{n}{n_1})$ where n_1 is square-free and

$$n_1\geqslant\frac{n}{(\log x)^2}. \tag{40}$$

Using (40) we have

$$\phi(n)=\phi\left(n_1\cdot\frac{n}{n_1}\right)\leqslant\frac{n}{n_1}\phi(n_1)\leqslant(\log x)^2\phi(n_1). \tag{41}$$

As a result, combining (41) with the fact that $\lambda(n)\geqslant\lambda(n_1)$, we deduce

$$\begin{aligned}\frac{\phi(n)}{\lambda(n)}&\leqslant\frac{(\log x)^2\phi(n_1)}{\lambda(n_1)}\leqslant(\log x)^2\prod_{\substack{pq\mid n_1\\ p\neq q}}(p-1,q-1)\\ &\leqslant(\log x)^2\big((\log x)^{(1+\epsilon)}\big)^{\binom{\omega(n)}{2}}\leqslant\exp\big(O\big((\log\log x)^3\big)\big).\end{aligned} \tag{42}$$

It follows from (42) that

$$\log\left(\frac{\phi(n)}{\lambda(n)}\right)=O\big((\log\log x)^3\big) \tag{43}$$

when n is not in A. Gathering (39) and (43) together, we obtain

$$\begin{aligned}\sum_{n\leqslant x}\frac{D(\mathbb{Z}_n^*)}{\lambda(n)}&\leqslant\sum_{n\leqslant x}\left(1+\log\left(\frac{\phi(n)}{\lambda(n)}\right)\right)\\ &=\sum_{n\leqslant x}1+\sum_{n\in A}\log\left(\frac{\phi(n)}{\lambda(n)}\right)+\sum_{n\notin A}\log\left(\frac{\phi(n)}{\lambda(n)}\right)=O\big(x(\log\log x)^3\big).\end{aligned}$$

This completes the proof of Theorem 4. □

Remark. The average value of the function $\log(\frac{\phi(n)}{\lambda(n)})$ played a key role in the proof Theorem 4. In connection with this, we should mention that a very detailed study on the distribution of prime divisors of the quotient $\frac{\phi(n)}{\lambda(n)}$, which is roughly a measure of how far the group of reduced residues is from being cyclic, was recently done by Banks, Luca and Shparlinski [3]. Although only upper bounds on this quotient were needed for Theorem 4, obtaining lower bounds and the true order of growth of the average

$$\frac{1}{x}\sum_{n\leqslant x}\log\left(\frac{\phi(n)}{\lambda(n)}\right)$$

is an interesting problem on its own right. It is known by the work of Banks, Luca and Shparlinski [3] that there exists some positive constant c such that almost all $n \leqslant x$ have

$$\gg \frac{\log\log x}{q}$$

prime factors p satisfying $p \equiv 1 \pmod{q}$ and this holds for all primes q with

$$q \leqslant \frac{c\log\log x}{\log\log\log x}.$$

Let $L(n)$ denote the least common multiple of numbers of the form $p-1$ for all prime divisors p of n. As a consequence we have

$$\frac{\phi(n)}{\lambda(n)} = \frac{\prod_{p|n}(p-1)}{L(n)} \geqslant \prod_{\substack{q \leqslant \frac{c\log\log x}{\log\log\log x} \\ q \text{ prime}}} q^{\frac{c'\log\log x}{q}}$$

for some $c' > 0$ and for almost all $n \leqslant x$, where the product on the left is taken over all prime divisors of n. Using Mertens' estimate, we have

$$\log\left(\frac{\phi(n)}{\lambda(n)}\right) \gg \log\log x \sum_{q \leqslant \frac{c\log\log x}{\log\log\log x}} \frac{\log q}{q} \gg \log\log x \cdot \log\log\log x$$

for almost all $n \leqslant x$ and consequently that

$$\frac{1}{x}\sum_{n \leqslant x} \log\left(\frac{\phi(n)}{\lambda(n)}\right) \gg \log\log x \cdot \log\log\log x.$$

This lower bound seems to be close to the true order of magnitude of the average of $\log(\frac{\phi(n)}{\lambda(n)})$ because of (35).

ACKNOWLEDGEMENT

The author is grateful to the referee for many valuable comments, suggestions and criticisms especially for pointing out improvements, bringing to his attention the important work of Banks, Luca and Shparlinski [3] and the remark following the proof of Theorem 4.

REFERENCES

[1] Alford W.R., Granville A., Pomerance C. – There are infinitely many Carmichael numbers, Ann. Math. **139** (3) (1994) 703–722.

[2] Baker R.C., Schmidt W.M. – Diophantine problems in variables restricted to the values of 0 and 1, J. Number Theory **12** (4) (1980) 460–486.

[3] Banks W.D., Luca F., Shparlinski I.E. – Arithmetic properties of $\frac{\varphi(n)}{\lambda(n)}$ and the structure of the multiplicative group modulo n, Comment. Math. Helv. **81** (1) (2006) 1–22.

[4] Chapman S.T., Freeze M., Gao W.D., Smith W.W. – On Davenport's constant of finite abelian groups, Far East J. Math. Sci. **5** (1) (2002) 47–54.
[5] Chapman S.T., Freeze M., Smith W.W. – Minimal zero-sequences and the strong Davenport constant, Discrete Math. **203** (1–3) (1999) 271–277.
[6] Davenport H. – Proceedings of the Midwestern Conference on Group Theory and Number Theory, Ohio State University, 1966.
[7] Delorme C., Ordaz O., Quiroz D. – Some remarks on Davenport constant, Discrete Math. **237** (1–3) (2001) 119–128.
[8] Dimitrov V. – On the strong Davenport constant of nonabelian finite p-groups, Math. Balkanica **18** (1–2) (2004) 131–140.
[9] Doyon N., Luca F. – On the local behavior of the Carmichael λ-function, Michigan Math. J. **54** (2) (2006) 283–300.
[10] Erdös P. – On the integers having exactly K prime factors, Ann. Math. **49** (1948) 53–66.
[11] Erdös P., Pomerance C., Schmutz E. – Carmichael's lambda function, Acta Arith. **58** (4) (1991) 363–385.
[12] Ford K. – The distribution of integers with a divisor in a given interval, Ann. Math., to appear.
[13] Ford K., Hu Y. – Divisors of the Euler and Carmichael functions, Preprint.
[14] Gao W.D. – On Davenport's constant of finite abelian groups with rank three, Discrete Math. **222** (1–3) (2000) 111–124.
[15] Gao W.D., Lin H.F. – Some estimates of Davenport's constant, J. Math. Res. Exposition **16** (2) (1996) 297–300.
[16] Geroldinger A., Schneider R. – On Davenport's constant, J. Combin. Theory Ser. A **61** (1) (1992) 147–152.
[17] Halberstam H., Richert H.-E. – Sieve Methods, London Mathematical Society Monographs, vol. 4, Academic Press, London, 1974.
[18] Hall R.R., Tenenbaum G. – Divisors, Cambridge Tracts in Mathematics, vol. 90, Cambridge University Press, Cambridge, 1988.
[19] Hardy G.H., Ramanujan S. – The normal number of prime factors of a number n, Quart. J. Math. **48** (1917) 76–92.
[20] Hardy G.H., Wright E.M. – An Introduction to the Theory of Numbers, 5th ed., Clarendon Press, Oxford University Press, New York, 1979.
[21] Ivić A. – The Riemann Zeta Function, The Theory of the Riemann Zeta Function with Applications, Wiley-Interscience, New York, 1985.
[22] Luca F., Sankaranarayanan A. – On the moments of the Carmichael λ function, Acta Arith. **123** (4) (2006) 389–398.
[23] Luca F., Shparlinski I.E. – Average multiplicative orders of elements modulo n, Acta Arith. **109** (4) (2003) 387–411.
[24] Mazur M. – A note on the growth of Davenport's constant, Manuscripta Math. **74** (3) (1992) 229–235.
[25] Meshulam R. – An uncertainty inequality and zero subsums, Discrete Math. **84** (2) (1990) 197–200.
[26] Montgomery H.L., Vaughan R.C. – The large sieve, Mathematika **20** (1973) 119–134.
[27] Narkiewicz W., Śliwa J. – Finite abelian groups and factorization problems—II, Colloq. Math. **46** (1) (1982) 115–122.
[28] Nicolas J.L. – Petites valeurs de la fonction d'Euler, J. Number Theory **17** (3) (1983) 375–388.
[29] Olson J.E. – A combinatorial problem on finite abelian groups I, J. Number Theory **1** (1969) 8–10.
[30] Olson J.E. – A combinatorial problem on finite abelian groups II, J. Number Theory **1** (1969) 195–199.
[31] Sathe L.G. – On a problem of Hardy on the distribution of integers having a given number of prime factors I, J. Indian Math. Soc. (N.S.) **17** (1953) 63–82.
[32] Sathe L.G. – On a problem of Hardy on the distribution of integers having a given number of prime factors II, J. Indian Math. Soc. (N.S.) **17** (1953) 83–141.
[33] Selberg A. – Note on a paper by L.G. Sathe, J. Indian Math. Soc. (N.S.) **18** (1954) 83–87.
[34] Skalba M. – On the relative Davenport constant, European J. Combin. **19** (2) (1998) 221–225.

[35] Tenenbaum G. – Introduction to Analytic and Probabilistic Number Theory, Cambridge Stud. Adv. Math., vol. 46, Cambridge University Press, Cambridge, 1995.
[36] Van Emde Boas P. – A combinatorial problem on finite abelian groups II, Report ZW-1969-007, Math. Centre Amsterdam.
[37] Van Emde Boas P., Kruyswijk D. – A combinatorial problem on finite abelian groups III, Report ZW-1969-008, Math. Centre Amsterdam.